**Fancy Bear**

APT28 // Pawn Storm // Sofacy Group // Sednit // STRONTIUM

Fancy Bear is the pseudonym given to an advanced nation-state group thought to operate out of Russia, likely in conjunction with Russian government and intelligence. They are thought to be the group that hacked into the DNC and released Presidential Candidate Hillary Clinton’s emails in late 2016.

Fancy Bear, also popularly known as APT28 and the Sofacy Group, specializes in politically motivated espionage for the express purpose of stealing national security related secrets as well as influencing political processes abroad. They are extremely adept actors, well-funded and almost definitely nation-state backed.

From an attribution perspective, Fancy Bear’s targets align with what one would expect. These targets have included Eastern European governments and militaries, NATO, and US defense contractors. They also seem to be incredibly advanced in terms of propaganda and media/political influence. The malware used by this group was also compiled using Russian language settings, with timestamps consistent with Russian working hours, specifically Moscow and St. Petersburg.

Fancy Bear has been in action since at least as far back as 2007. Their efforts have been concerted specifically around former soviet republics, particularly Georgia, as well as security organizations like NATO and US defense contractors. Their malware was propagated via target-specific spear-phishing emails in the language of their target, usually containing weaponized decoy files. These decoy files were sent to government employees at the Ministry of Defence and Ministry of Internal Affairs of the Georgian government, which would align with Russia’s interests after the Russia-Georgia war and Georgia’s increased cooperation with the West. Fancy Bear also targeted a controversial journalist that wrote about Georgian issues, using the same spear-phishing methods and malware.

The targeted journalist is especially interesting, considering APT-28 being a nation-state sponsored group. The government and security targets make sense, but the targeted journalist would only be attacked if the actor behind the attacks had special interest in public opinion and propaganda. This is right up the Propaganda Empire’s alley, and is more indicative of Russia, or perhaps China, than any other known threat actor.

APT28 also set up fake domains that very closely mirrored legitimate ones. In one attack, they set up a domain that mimicked a Chechen-focused news website, while another mimicked a login page used by Armenian military personnel. They often mirrored events that were in the news at the time, including a document carrying APT 28 malware that detailed hostilities at the crash site of MH-17.

Fancy Bear actors registered domains that mimicked those of Eastern European targets, meaning that their campaign may have included more than efforts that were already detected. Their targeting of Eastern European nations, as well as NATO, shows that in contrast to their APT1 Chinese counterparts, APT28 was focused on insider political secrets instead of intellectual property. Insider information on NATO and Eastern European nations would give Russia an upper hand and early warning of NATO’s future plans and their adversaries prospective ideas in the contested former-Soviet region.

The targets obviously point to nation-state backing, and the intelligence required to refine the decoy documents and phishing emails also indicates a high-level of operational intelligence obtained by the actors before the attacks were launched. The malware itself carried signs of a professional, team-based development environment, employing reverse-engineering evasion and particular attention to stealth and constant, modular improvement. Obfuscated strings and a well-updated framework indicates that the actors were focused on long-term presence and constant improvement rather than a smash-and-grab attack.

**DNC Hack**

Fancy Bear employed characteristically advanced malware and TPPs to infiltrate the DNC. They employed open-source tools found online as well as custom-crafted malware, downloaders, and tunneling software to hide their presence and exfiltrate data. The attack was carried out alongside, but seemingly completely unaware of, another Russian nation-state actor, Cozy Bear, showing Russia’s extreme interest in influencing and gaining information on the United States’ political system. Cozy Bear had infiltrated the network in 2015, a year before Fancy Bear, and used different but just as sophisticated tools and tactics against the DNC.

Fancy Bear, according to Crowdstrike CTO Dmitri Alperovitch, was after opposition research on the DNC network. This is an extremely interesting observation, for a multitude of reasons. The general consensus is that Russia’s influence on the 2016 election was intended to tip the scales in Donald Trump’s favor. As the attacks were largely targeted toward the DNC, as well as the fact that the political relationship between Donald and Vladimir is much closer to warm than that of the Russian oligarch’s attitude towards Hillary, this is an understandable conclusion to reach. This brings forth the following question: why was Russia trying to dig up dirt on their glorious leader’s pal?

My political opinion is that Russia saw Donald Trump as a controllable ally, one that is much easier to bring to heel than Hillary. Digging up dirt on the world-leader-to-be would bring Russia even more international control. While most analysts believe that the groups were competing for favor in a tense political rivalry between intelligence agencies, there is the possibility that they both simply had different missions: one to tip the scales in Donald’s favor, one to make sure Vlad had some good blackmail for when the Orange Man reached the White House.

Political analysis aside, analysis of malware used against the DNC matched malware used in the aforementioned campaigns by Fancy Bear, and the TTPs were also extremely similar. The two groups may have had different missions, and may have been entirely unaware of the other’s actions or presence, but the overall intention was clear: undermining the democratic process of the United States and tipping the scales in the former Soviet Union’s favor.